**2022년도 졸업프로젝트[Back-end]**

**팀이름: 황제펭귄**

주제: TLS를 구현을 통한 홈페이지 제작 및 보안 채널 로그인 기능 구현

|  |  |  |  |
| --- | --- | --- | --- |
| **작성자** | 정경재(수정:이유민) | **작성일자** | 2022.04.04 |

* **금일 진행 상황**

|  |  |
| --- | --- |
| **진행 상황** | **비고** |
| **질문 및 진행방식에 대한 논의**  **진행 중**  **완료** }  **3단 인증서 제작**   * **인증서 구성**   **1.RootCA생성 및 정보 입력**  1.Openssl req ‑x509 ‑newkey rsa:4096 ‑keyout EmperorPenguin\_key.pem ‑out EmperorPenguin\_crt.crt ‑sha256 ‑days 3650  -4096비트의 RSA-sha-256방식인 자체 사인 인증서 생성  -Key 파일명: EmperorPenguin\_key.pem  -인증서(CRT) 파일명: EmperorPenguin\_crt.crt  -만료기간 3650일    2.Challenge PassWord 및 각종 정보 입력하기  challenge password:865949    **2.SubCA 생성 및 정보입력** 텍스트이(가) 표시된 사진  자동 생성된 설명1**.**Openssl req -new -key SecurityGraduation\_Sub\_key.pem -out SecurityGraduation\_Sub\_csr.csr -sha256 4096  -4096비트의 sha-256 방식인 인증서 생성  -Key 파일명: SecurityGraduation\_Sub\_key.pem  -인증요청서(CSR) 파일명 SecurityGraduation\_Sub\_csr.csr  텍스트이(가) 표시된 사진  자동 생성된 설명  2.각종정보 입력하기  challenge password: 136987    3.RootCA소명 후 SubCA 인증서(CRT) 생성  openssl x509 -req -CA EmperorPenguin\_crt.crt -CAkey EmperorPenguin\_key.pem -days 3650 -set\_serial 1 -in SecurityGraduation\_Sub\_csr.csr -out SecurityGraduation\_Sub\_crt.crt -sha256 -extfile SubCA.ext -extensions server   1. 각종 정보 입력하기 텍스트이(가) 표시된 사진     자동 생성된 설명   **3.ServerCA생성**  1. KEY 생성  openssl genrsa -out SangmyungBank\_key.pem 4096  -4096 bit key 생성 텍스트이(가) 표시된 사진  자동 생성된 설명  2.CSR 생성  openssl req -new -key SangmyungBank\_key.pem -out SangmyungBank\_csr.csr -sha256  -Key 파일명: SangmyungBank\_key.pem  -CSR 파일명 SangmyungBank\_csr.csr    3.각종 정보 입력하기 Challenge Password: 640927 텍스트이(가) 표시된 사진  자동 생성된 설명  4.SubCA 소명 후 SangmyungBank\_.csr로 crt파일 생성  openssl x509 -req -CA EmperorPenguin\_crt.crt -CAkey EmperorPenguin\_key.pem -days 1825 -set\_serial 1 -in SangmyungBank\_csr.csr -out SangmyungBank\_crt.crt -sha256 -extfile Leaf.ext -extensions server 텍스트이(가) 표시된 사진  자동 생성된 설명  5.SangmyungBank\_crt.crt를 SangmyungBank\_key.pem와 결합해 .keystore로 변환  openssl pkcs12 -export -in SangmyungBank\_crt.crt -inkey SangmyungBank\_key.pem -out .keystore -certfile SecurityGraduation\_Sub\_crt.crt |  |
| * **특이사항 / 협업 사항** | |